CATALOGUE OF **RISK** INDICATORS

2024

Credit Institutions

MINISTERIO
DE ECONOMÍA, COMERCIO
Y EMPRESA

COMMISSION FOR THE
PREVENTION OF MONEY
LAUNDERING AND MONETARY
OFFENSES

INTRODUCTION

This document contains a list of risk indicators for money laundering and terrorist financing (hereinafter, ML/TF).

The purpose of this document is to assist regulated entities in complying with Law 10/2010 of April 28 on the prevention of money laundering and terrorist financing. Knowledge and use of these indicators can help improve the systems implemented by regulated entities to prevent and detect money laundering or terrorist financing transactions.

The presence in specific transactions of the indicators shown in this list does not necessarily imply the existence of money laundering or terrorist financing, which must in any case be assessed in the corresponding special review to be conducted by the regulated entity. However, the presence of these indicators can help the regulated entity identify the cases to be selected for the special review.

Likewise, the list of indicators provided below, duly adapted to the nature of the regulated entity's activity, may assist the entity in developing its own catalogue of transactions that may be related to money laundering or terrorist financing.

Law 10/2010 of April 28 on the Prevention of Money Laundering and Terrorist Financing, in Article 2.1.a), establishes the status of obligated entities for credit institutions.

As indicated in the National Risk Assessment approved by the Commission of Anti-Money Laundering in 2020[1], updated in April 2024, this sector carries a **very high inherent risk**, since most of the monetary flows circulating through the financial system are channelled through credit institutions.

Consequently, the sector's size, number of customers, number of transactions and deposits, the economic volume of transactions, and its international reach make the credit institution sector highly attractive and, at the same time, highly vulnerable to ML/TF operations. The residual risk of the activities carried out is determined by the high degree of regulation, control, and supervision of this sector at the national level by the authorities, both in terms of prudential matters and ML/TF prevention. Furthermore, the credit institution sector has the greatest understanding of its preventive obligations and of the ML/TF risk operations that affect it.

This high level of risk awareness, both at the sectoral level and at the individual institution level, means that institutions develop and implement internal control policies and procedures for ML/TF prevention that include the evaluation and approval of their own risk assessments at the individual level. These internal control procedures, which include early warning systems, decision-making procedures, and customer onboarding policies, among other areas, are not static; rather, they are sufficiently flexible to appropriately address evolving ML/TF threats and, furthermore, must adapt swiftly to internal changes as well as external corporate processes such as mergers, acquisitions, or spin-offs.

The interaction of inherent and residual risks depending on the type of operations results in a different level of residual risk for each type of service or activity provided and for each individual entity; therefore, along with the description of the risk elements derived from common vulnerabilities in the sector described in the risk fact sheet, the specific risks posed by the various types of financial services provided must be taken into account.

[1] 1.1_public_summary_of_the_national_risk_analysis.pdf (tesoro.es)

Likewise, the European Union's Supranational Risk Assessment, the third edition of which was published in October 2022[2], classifies the risk in the sector as high or very high, depending on the product or service, specifically highlighting the importance of controls over clients with complex offshore structures and foreign clients from high-risk jurisdictions.

Among credit institutions, anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations require specific and enhanced safeguards for the private banking sector. Thus, in Article 11, Law 10/2010 of 28 April, establishes that obligated entities shall apply, based on a risk analysis, enhanced due diligence measures in situations that, by their very nature, may present a higher risk of money laundering or terrorist financing, with private banking activities being considered as such in all cases. Article 19 of the Regulations implementing the Act, approved by Royal Decree 304/2014 of May 5, provides similarly.

As indicated in the National Risk Assessment approved by the Commission for the Prevention of Money Laundering in 2020 and updated in April 2024, the very nature of private banking activities and the specific conditions under which they are conducted mean that these services carry a high risk of being used for ML/TF purposes. This risk stems from the complexity of fund and asset management operations, the difficulty in identifying beneficial owners, the high returns that can be generated for both the client and the manager, and the frequency of cross-border transactions and investments, including, on occasion, transactions and investments in which offshore financial centers may be involved, offshore jurisdictions, and other higher-risk countries.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344

At the international level, FATF developed a risk-based guidance for the banking sector[3] in 2014. Furthermore, the EBA published updated guidance on ML/TF[4] risk factors in 20214. This guidance also includes sector-specific guidelines for wealth management, directly related to banking activities[5].

This catalogue has been prepared by the Commission for the Prevention of Money Laundering and Monetary Offenses, in the exercise of its functions, in collaboration with industry associations, with the aim of assisting regulated entities in complying with their obligations. This catalogue of risk indicators, therefore, seeks to help regulated entities fulfill their preventive obligations, an objective that Directive (EU) 2024/1640 pursues in Article 26(1)(a) when it urges Financial Intelligence Units (FIUs) to provide information regarding *"the types of transactions or activities that present a significant risk of money laundering, its underlying crimes, and terrorist financing"*. This list is an update of the one prepared in 2013 by the Commission for the Prevention of Money Laundering and Monetary Offenses in collaboration with the sector, which has been prompted by developments in operations and risks.

This catalogue is divided into two sections. The first section, titled *"General Indicators"*, includes indicators that, in principle, can be identified by any type of obligated entity. The second section, titled *"specific indicators"*, others are identified that refer to specific activities carried out only by certain types of regulated entities.

---

[3] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf

[4] https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2023/EBA-GL-2023-03/1061654/Guidelines%20ML%20TF%20Risk%20Factors_consolidated.pdf.pdf?retry=1

[5] https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2023/EBA-GL-2023-03/1061654/Guidelines%20ML%20TF%20Risk%20Factors_consolidated.pdf.pdf?retry=1

The indicators shown in the list are only a selection of the many indicators that can be found in money laundering, its various types of underlying crimes, and terrorist financing. An effort has been made to select those that are most evident and general. For indicators related to more specific typologies, the regulated entity may refer to various publications by organizations and institutions that conduct studies on specific typologies, revealing the most frequent indicators. Likewise, it is recommended that the regulated entity add to the suggested list other indicators derived from cases it analyzes on its own and assesses as linked to terrorist financing, money laundering, or their underlying criminal activities.

Finally, the development of this catalogue has been accompanied by the preparation of a Report on the Most Commonly Used Criminal Typologies Today, classified according to the primary underlying crime to which they are typically linked. The purpose of this document is to facilitate the work of obligated entities, insofar as a better understanding of the ways in which threats manifest in this area (drug trafficking, organized crime, corruption, etc.) can help improve the systems implemented by obligated entities to prevent and detect ML/TF transactions.

GENERAL RISK INDICATORS

In the process of conducting due diligence

In the interaction between the regulated entity and its customer regarding due diligence, certain factors may arise that, while not preventing the completion of due diligence, are relevant in the context of detecting money laundering or terrorist financing. These include the following:

- In general, the customer's refusal to provide information to the regulated entity during the course of the due diligence process.
- The customer's use of general terms such as "savings," "work," or similar expressions to inform the obligated entity about the source of their assets, in an attempt to avoid providing specific information about the nature of their employment, professional, or business activities.
- The withdrawal of a transaction, or the modification of any of its characteristics (such as the amount), when the regulated entity requests that the customer provide additional documentation or information.
- The behaviour of customers who demonstrate a high level of knowledge of anti-money laundering regulations and an unusual interest in the procedures implemented by the regulated entity to ensure compliance.
- A request made by the customer to the obligated party not to comply with any of its due diligence obligations or with the proper recording of transactions, usually linked, explicitly or implicitly, to or not of new transactions or to the

maintenance of the business relationship.

- The client's demand for unusually high levels of confidentiality or discretion.
- Providing addresses as a primary residence that do not correspond to residential properties or premises for exclusive use, such as business centers, hotels, etc., when this is inconsistent with the regulated entity's knowledge of the customer, or with the number, amount, or profile of their transactions.
- A discrepancy between the country of residence declared by the customer to the obligated party and the country of the address the customer provides for mailing correspondence, the country of the contact phone number provided, or the country of the domain for their email account or website.
- Customers whose behaviour indicates adherence to radical extremist ideologies or who exhibit violent tendencies.
- Customers whose tax identification number (NIF) has been revoked at the time of conducting transactions or establishing business relationships, including those who are beneficial owners or directors of companies.

In remote transactions

By conducting remote transactions without direct contact with the regulated entity, it is possible to conceal the fact that those carrying out the transactions are not the individuals who have formally contracted with the regulated entity. Concealing the identity of the true person responsible for or the beneficial owner of the transactions is very common in ML/TF processes. The following are some indicators:

- Customers who consistently avoid conducting transactions in person and instead carry out remotely transactions that are typically conducted in person.

- Access to the regulated entity's online services through the use of VPN services, proxy servers, or other mechanisms that conceal or hinder the geolocation of transactions.
- Frequent changes in IP addresses or devices when the same customer accesses the regulated entity's online services, without a justifiable reason.
- Attempts to open accounts or purchase products from IP addresses or devices previously used by customers other than those who intend to appear as the holders of the new account or the new product to be purchased, and without any apparent relationship between those former customers and the new customer.
- Attempts to purchase products remotely using the identity information of a customer already known to the regulated entity, when contact information is provided that does not match the information the regulated entity has on file for the known customer, or when there are other reasons to suspect that the customer's identity is being impersonated.
- Repeated access to the regulated entity's online services by the same customer from the same IP address, whose geolocation does not correspond to the location the customer has reported as their usual residence.
- Access to the regulated entity's online services by the same customer, within a short period of time, from several different locations that—based on their geolocation—are so far apart that it would be impossible to travel from one to the other in the time between connections.

On the Relocation of Transactions

As a result of economic globalization, international transactions are becoming increasingly common. However, on occasion, the international component is sought out intentionally, in an artificial manner, to distribute the elements of a single transaction across different jurisdictions and thus prevent the authorities of a single country from having a comprehensive understanding of the transaction. Such practices are common in AML/CFT processes. The following are some indicators:

- The execution of transactions that indicate or suggest the possibility that the regulated entity's customer has assets abroad, when this is inconsistent with the regulated entity's knowledge of the customer.
- The purchase of products in Spain by foreign individuals or legal entities, when there are no logical reasons for such purchases to be made in our country.
- The operation of accounts domiciled in Spain (typically at branches in locations near the border with Spain or Portugal) that are limited to the mass receipt of transfers or other types of income originating in the other country, with the funds subsequently being disposed of through cash withdrawals or transfers to the same or another country.
- In general, transactions involving structures spanning multiple jurisdictions, without a justifiable reason.
- The use of corporate structures in which the beneficial owner, the directors, or the company are located in different jurisdictions, without a justifiable reason.
- The use of corporate structures in which different companies from different jurisdictions own one another, without a justifiable reason.

Acting on behalf of a third party

Individuals involved in money laundering schemes, their underlying crimes, and/or terrorist financing naturally seek to conceal their identity. To do so, they may use other individuals as frontmen who, acting on their instructions, interact with regulated entities and formally appear as the parties to the transactions. Below are some indicators that may suggest the regulated entity's customer is acting on behalf of another person:

- Cases in which a person acts, de facto or de jure, on behalf of the customer, when, based on the prevailing circumstances and the conduct of both parties, the regulated entity understands that decisions regarding the transactions or the business relationship are made by the representative, not the represented party.
- Cases in which a person, whether a known customer or a professional, acts as an introducer of a new customer to the regulated entity, and it is the introducer who negotiates the new customer's position with the regulated entity.
- A contract entered into by a new client who provides the same address, phone number, or email address as a previous client, with whom they apparently have no relationship, and who carries out similar transactions.
- Cases in which it is observed that, in practice, one client is replaced by another, such that when the first client terminates a business relationship, a new client—who formally appears to be independent of the previous one—establishes a new business relationship involving the same type of transactions.

- Successive contracting with several companies, sometimes represented by the same individuals, such that once the transaction or business relationship of one of them ceases, another takes its place and carries out the same type of operations as the previous company, even with the same counterparties.
- The actions of several clients acting as a group, such that each of them carries out a transaction with characteristics similar to those of the others, especially if it is observed that a third party, or one of them, is giving instructions to the others.
- Cases of remote onboarding where it appears that the new client is being assisted by a third party, for example, during the remote identification process via videoconference.
- The existence of several customers with no apparent connection to one another who provide the same address, phone number, or email address, or who conduct online transactions using the same IP address.
- Changes to a customer's contact information (phone number, email address) shortly after the account is opened or just before they begin conducting transactions.

Splitting of Transactions

In many AML/CFT processes, the high volume of transactions can be conspicuous. Furthermore, exceeding certain thresholds may require the regulated entity to adopt enhanced due diligence measures or report information to the authorities. For this reason, transactions are very often split into several smaller ones, typically in the names of different individuals, so that each one is less conspicuous and does not trigger action by the regulated entity. The following are some indicators that a transaction has been split into several:

- The execution by a single customer, or by several acting in a coordinated manner, of multiple transactions of the same type, with the same origin and destination, consecutively, or within a short period of time, when, had the transaction been carried out in a single transaction for its total amount, the customer would have been required to provide additional information or documentation to the obligated entity.
- The purchase by the same person of many products, whether they are used simultaneously (the products are active at the same time) or successively (when one is cancelled, another is purchased), carrying out a similar transaction.
- Cases in which a total payment is split into several payments, theoretically to benefit the payer, yet the time intervals between each payment are so short that they offer no practical advantage.

Regarding individuals or legal entities and beneficial ownership

Individuals or legal structures involved in money laundering processes and their underlying crimes logically seek to conceal their identity. One form of concealment is the use of individuals or legal structures in which corporate positions and beneficial ownership are formally held by front men. Below are some indicators related to practices that are more closely linked to money laundering, although it is more difficult to find such indicators in terrorist financing offenses:

- Individuals or legal entities that experience frequent changes in the identification of their beneficial owner.
- Individuals or legal entities that declare a change in beneficial ownership without corresponding changes in their management or representatives.

- When there is evidence of a transfer of ownership of the company, but its representatives wish to rely on a beneficial ownership declaration made prior to the transfer.
- Individuals or legal entities that, in commercial practice, appear to be represented by persons who are neither their legal representative nor their beneficial owner.
- Individuals or legal entities whose beneficial ownership declaration is inconsistent with the information and documentation collected by the reporting entity.
- Appointment of directors who clearly lack the necessary competence or suitability to perform the duties of the position.
- Use of companies, or other types of legal persons or structures, incorporated in foreign countries whose legal regime permits the use of nominee shareholders, or allows the identification of the partner in a private document, such that in practice it is impossible to verify beneficial ownership through documentation.
- A person who regularly appears in the incorporation or establishment of legal entities or structures that are immediately transferred to another person.
- The simultaneous incorporation or creation of several legal entities or structures involving the same natural or legal person, where there is no economic rationale or where anomalous circumstances exist.

Place and time of transactions

Some indicators that take into account the place and time in which transactions are carried out include:

- Contracting a service or conducting a transaction in person at a location far from the customer's usual residence, when alternatives exist that would avoid the trip and there are no justifiable reasons for it.
- A customer repeatedly and systematically conducting transactions during peak hours at the regulated entity's premises, when it appears that this is an attempt to hinder the regulated entity's ability to perform due diligence or record the transactions.
- A customer's request that the transaction be completed within an unusually short timeframe, without a reasonable explanation for expediting the transaction, when it appears that this is an attempt to hinder the regulated entity's performance of due diligence.

Employees and Agents

Criminal organizations engaged in ML/TF and their underlying criminal activities have significant financial resources and may bribe employees and agents of regulated entities to fail to apply adequate due diligence, fail to properly record transactions, or fail to report to the authorities. The following are some indicators that an employee or agent may have been bribed:

- An employee's unjustified refusal to be promoted, take vacation, or make other changes that would result in losing direct contact with their clients.
- An employee displaying a standard of living higher than what would be expected given their income, without a justifiable reason.

- An employee or agent who experiences a sudden increase, without a logical explanation, in the number of clients, the number or amount of their transactions, or the profile of those transactions.
- The concentration of transactions by an employee's or agent's customers on dates or at times that are normally periods of low public activity, without any justifiable cause.
- The agent's reluctance to comply with the regulated entity's anti-money laundering (AML) and countering the financing of terrorism (CFT) measures, claiming that the measures established by other regulated entities for which they also act as an agent are more lenient.

Possible connection to ML/TF criminal activities

On occasion, the link between the customer or their transactions and criminal activities may be inferred by the regulated entity from its relationship with the authorities or may even be in the public domain. Some indicators are noted below:

- Transactions by customers regarding whom requests or inquiries for information are received from national authorities, in the context of an investigation into criminal activities.
- Transactions by customers directly or indirectly related to other customers regarding whom requests or inquiries for information have been received from national authorities in the context of criminal investigations.
- Transactions involving customers for whom there is public information linking them to criminal activities.
- Client transactions that involve the same type of trading and the same counterparties as those of other clients whose transactions were analyzed and

concluded to have a possible link to money laundering, or to underlying criminal activities, and/or the financing of terrorism.

- Customers subject to international sanctions, and persons associated with them.

RISK INDICATORS IN SPECIFIC ACTIVITIES

In cash transactions

- The execution of a cash payment when, due to the amount, the nature of the transaction, or other circumstances, the use of cash was not expected.
- Account activity involving cash deposits made by different individuals or multiple deposits by the same individual, without a justifiable reason.
- The acquisition of bearer payment instruments (bank checks, electronic money, traveller's checks, etc.) in exchange for cash, especially when the instruments are not presented for collection within a reasonable period of time.
- Cash deposits where, due to their being split into smaller amounts, the identity of the person making them is unknown, or when such identification is hindered by the customer's avoidance of the regulated entity's offices, the use of ATMs, or the unnecessary use of a cash-in-transit company's services.

- Cash deposits that are immediately followed by the transfer of their value abroad; or deposits that are immediately followed by the withdrawal of funds from ATMs abroad.
- Cash deposits immediately followed by card payments to cryptoasset service providers, in Spain or abroad.
- Cash withdrawals charged to balances generated through POS transactions, when the frequency and amounts suggest a scheme involving cash delivery in exchange for a charge to the card account.
- Cash deposits made to associations, foundations, or other entities, when it is reported that the cash comes from fundraisers or collections, and the type of banknote used in the deposit is inconsistent with this.
- Cash deposits in which counterfeit bills appear more frequently than usual.
- Fundraising operations with diverse sources (online platforms, PSCA, payment platforms, etc.) where the proceeds are withdrawn in cash.
- Cash deposits consisting of banknotes that are very dirty, damp, moldy, or have a strange odor.
- Exchanging large quantities of small-denomination bills for large-denomination bills.
- Frequent or significant exchanges of euros for foreign currency or vice versa that are not justified by the customer's professional or commercial activity.

In account and deposit operations

- Accounts that experience an unexpected increase in the number of transactions, or in the amount of these transactions, or significant changes in the type of transactions recorded, without this being consistent with the regulated entity's knowledge of its customer.
- Accounts that remain inactive for a period of time and then suddenly begin to show intense activity, without any known cause to justify it.
- Accounts that channel funds received from a single originator to multiple beneficiaries, or that receive funds from multiple originators to a single beneficiary, without this being consistent with the regulated entity's knowledge of its customer.
- Accounts for which, due to the coincidence of the origin or destination of funds, the type of transaction, connections, devices, or for any other reason, it can be inferred that they are continuations of other accounts previously closed by the regulated entity for AML/CFT prevention reasons.
- Accounts held by individuals who, having stated that the purpose of the account is to conduct personal transactions, show intensive activity involving collections and payments with third parties but do not record domestic transactions (direct debit of bills, rent or utility payments, small card payments at merchants, etc.)
- Accounts whose sole activity is the receipt of fund transfers from third parties, the proceeds of which are immediately disbursed through cash withdrawals, international transfers, or transfers to cryptoasset service providers.
- Payment accounts that record transactions involving the receipt of transfers from cryptoasset service providers immediately following the withdrawal of cash funds or the issuance of transfers to third parties.

- Accounts in connection with which the regulated entity frequently receives requests for the reversal or cancellation of transactions, especially if the requester cites reasons of fraud.

  Payment accounts whose sole or almost sole activity is the receipt of one or more transfers of funds from third parties, the amount of which is immediately disposed of through cash withdrawals, transfers abroad, or transfers to cryptoasset service providers.

- Accounts of Publicly Responsible Persons that receive transfers from third parties without a commercial rationale.

- Customer accounts that, for no apparent business reason, are used to purchase airline tickets for third parties traveling to countries at risk of terrorism or linked to human trafficking.

- Accounts with deposits indicating they may be used for fundraising for alleged charitable causes, especially if the account is for personal use and/or if the deposits are immediately withdrawn in cash.

- Accounts from which, without justifiable reason, weapons or dual-use goods are purchased that could be used in terrorist attacks or in a war context (ammunition, explosive materials or their precursors, military supplies such as clothing, optical or electronic equipment, satellite phones, etc.).

In payment transactions

- Fund transfers where the beneficiary indicated by the payer does not match the payee account holder.
- Fund transfers in which the payment descriptions provided by the payer are inconsistent with the declared activity or with the operational history of the receiving account holder.
- Fund transfers in which the payment descriptions refer to illicit or prohibited activities, or to payment for goods such as drugs, weapons, information, etc.

In loan transactions

- Transactions in which loans have been obtained or are being sought with collateral provided, directly or indirectly, through cash.
- Transactions in which loans secured by assets in other jurisdictions have been obtained or are being sought, particularly in countries where it is difficult to determine whether the customer has legitimate ownership of the collateral, or where the identity of the parties securing the loan is difficult to verify.
- Early repayment of the loan within a short period of time, when it may be reasonable to conclude that the loan was unnecessary, either because the borrower is not using the funds for the stated purpose or because there is reason to suspect that the borrower already had the funds available to make the repayment.
- Loans guaranteed by individuals whose relationship with the lender is unclear, especially when the loan goes unpaid and the guarantors are left to cover the repayment.

- Loans between individuals in which, due to the lack of collateral for the lender, non-payment, or any other circumstance, there is suspicion that the lender and borrower acted in collusion and the loan is a sham.
- Applications for financing transactions in which the customer demonstrates their ability to pay the lender using funds not declared for tax purposes.
- Clients who show a complete lack of interest in the details of loan repayment, especially in the case of quick, small-amount loans.

In private banking transactions

- Changes in the customer's tax residence without a logical or substantiated justification.
- A customer's refusal to provide the regulated entity with information regarding their accounts and products at institutions located in other jurisdictions, particularly if those institutions belong to the same financial group as the regulated entity.
- Clients who show a lack of concern for the returns on their investments, ordering sales at significant losses, or making investment decisions that are out of the ordinary.
- Executives, managers, and employees who, in an effort to provide personalized service to their client portfolio, deviate from the regulated entity's control procedures, especially if there is suspicion that this was suggested by the client.
- Cross-border arrangements in which assets are deposited or managed at another financial institution, whether within the same financial group or outside it, especially when the other financial institution is headquartered in a jurisdiction associated with a higher risk of ML/TF.

Transactions involving crypto-assets

- Clients who purchase cryptoassets with fiat currency and then instruct that their value be transferred to self-custody wallets or to wallets managed by an unregulated service provider.
- Customers who receive funds from self-custodial wallets or wallets managed by an unregulated service provider and intend to convert them into fiat currency.
- Customers who receive or send funds from services that, acting as transaction mixers or otherwise, seek to obscure the traceability of transactions.
- Wallets that aggregate funds from a large number of theoretically independent customers within a short period of time and that, nevertheless, connect to the regulated entity's platform from the same IP address.
- Wallets that aggregate significant funds received from a number of small transactions suspected of being related to peer-to-peer (P2P) exchanges or similar activities.
- Customers who receive funds from wallets whose addresses appear in open-source data linked to commercial activities inconsistent with the regulated entity's knowledge of the customer, or to illicit businesses advertised on the dark web.
- Transactions involving crypto-assets that contain messages referring to illicit activities or the purchase of goods such as drugs, weapons, information, etc.
- Customers who receive a high volume of cryptoassets in their wallets that is inconsistent with the information provided to the regulated entity or with their operational history.
-

- Customers who inform a regulated entity that the source of their assets, or of the funds used in a transaction, are profits from investments in cryptoassets, when the information and documentation provided does not allow for the traceability of the transactions through which the investment was made to be identified or for the profits obtained to be verified.

Securities Transactions

- Changes to a customer's information, followed by changes to their operating instructions that may indicate a hidden change in the ultimate ownership or control of an account.
- Frequent changes in the accounts used by the same client, with the aim of hindering the tracking of their transactions.
- Submission of securities lending agreements or other transactions involving a change of ownership to jurisdictions that hinder or prevent the investment firm from obtaining information regarding the successful completion of the transaction, when such submission is not justified.
- Instructions to disburse the proceeds from the settlement of transactions to third parties other than the account holder, without any apparent economic rationale.
- Fund transfers issued from a significant number of accounts and received by an investment fund (or by several funds managed by the same manager) for the subscription of shares in the name of the same client.
- Transactions involving the design or request by the client for the design of OTC structures (custom-designed transactions between counterparties not traded on organized secondary markets), with or without the use of derivatives, where such use has no apparent lawful or economic purpose.

- Instructions for the settlement of transactions that deviate from normal, customary, or logical patterns from a market practices perspective (for example, the use of securities lending for settlement without the loan being repaid—whether or not collateral exists—when the characteristics of the client and their ordinary or reasonably expected operations do not provide a clear rationale for such a transaction).
- Participation in financial swap agreements on the over-the-counter (OTC) market, and subsequent settlement using funds of illicit origin.
- Purchases and sales of over-the-counter (OTC) securities where the means of payment cannot be traced or where there is a lack of substantive information necessary for traceability.
- Transfers of securities to or from high-risk jurisdictions or tax havens without a clear economic justification.
- Concerted actions by two or more parties (or through a single authorized representative) to transfer funds among themselves under the guise of proceeds from market transactions (e.g., derivatives markets through a member's daily account and subsequent allocation to the accounts of the parties involved).



September 2024

www.tesoro.es

secretariaICMC@economia.gob.es

Paseo del Prado 6, 28014, Madrid